

RECOVERING AFFINE CURVES OVER FINITE FIELDS FROM L -FUNCTIONS

JEREMY BOOHER AND JOSÉ FELIPE VOLOCH

ABSTRACT. Let K be the function field of a curve over a finite field of odd characteristic. We investigate using L -functions of Galois extensions of K to effectively recover K . When K is the function field of the projective line with four rational points removed, we show how to use L -functions of a ray class field to effectively recover the removed points up to automorphisms of the projective line. When K is the function field of a plane curve, we show how to effectively recover the equation of that curve using L -functions of Artin-Schreier extensions of K .

1. INTRODUCTION

Let K be a global field. The zeta function of K is an important invariant of K , encoding information about the places of K . By classical work of Gassmann, the zeta function of K alone does not determine K ; for example, Gassmann produces non-isomorphic number fields with the same zeta function [Ga&26]. Similarly, Tate has shown that two function fields have the same zeta function if and only if the Jacobians of the corresponding curves are isogenous [Tat66]. It is natural to ask if additional information of a similar nature helps.

Question 1.1. *Do zeta functions of Galois extensions of K (or L -functions for particular characters of the Galois group) suffice to determine K up to isomorphism? What kind of extensions are needed? Can this be done explicitly?*

There has been a number of recent papers addressing instances of this question.

- For example, [CdSL⁺19] proves that a global field can be recovered from its abelian L -functions. This requires a way to identify characters of two fields; more precisely, they prove two global fields are isomorphic if there is an identification of the groups of characters of their Abelianized absolute Galois groups preserving L -functions.
- We have shown that function fields of curves of genus at least two can be recovered from L -functions of unramified characters [BV20].
- Another approach is to attempt to recover extensions of a fixed global field from a few well-chosen L -functions. For number fields, see [LR] and the references therein, while [Sol] considers extensions of a fixed function field. A key difference is that all number fields are natural extensions of \mathbb{Q} , while function fields can be given as extensions of the rational function field in different ways and, in general, there is no canonical choice.

These results can all be seen as attempts to use limited information about the absolute Galois group of a global field to recover it. (Uchida and Neukirch have shown that the absolute Galois determines a global field [Neu69, Uch76, Uch77].)

Our goal is to study these questions for function fields of curves over finite fields with the goal of explicitly describing an effective, finite set of L -functions that characterizes the

curve. Our perspective is a bit different from the aforementioned results. We work with the function field of an affine curve with some fixed “shape” (for example a member of a family, or given by an equation of fixed degree) and we recover that “shape” using L -functions.

We work over the finite field \mathbb{F}_q , where q is a power of an odd prime p . Many of our arguments extend without change to characteristic 2 but a few do not. In some places, we will comment on the changes that would need to be made to extend the results but we do not systematically address the issue.

We first tackle the special case of the projective line minus four points. In this case, the function field is already determined and the goal is to determine the removed points using L -functions up to automorphisms of the projective line. We look at L -functions of a suitable class field (a ray class field for the function field giving an unramified cover of the projective line minus four points) and answer an analogue of a conjecture from [SV] in a strong form. Namely, we prove:

Theorem 1.2. *Let q be an odd prime-power and U be $\mathbb{P}_{\mathbb{F}_q}^1$ minus four \mathbb{F}_q -rational points. Then U can be recovered up to Frobenius twist from the L -functions associated to the maximal abelian extension of $\mathbb{F}_q(x)$ unramified over U and tamely ramified on its complement.*

We prove two version of this theorem. Theorem 3.17 (and Remark 3.20 for an exceptional case) shows this can be accomplished using the L -function of a single well-chosen character. Theorem 3.21 shows that if U and U' are of this form and there is an isomorphism between the Galois groups of appropriate ray class fields which identifies L -functions then U and U' are Frobenius twists. The proofs rely on obtaining information about the reductions of these L -functions modulo primes above p using the Cartier operator, making use of a result of Rück [Rüc86].

Remark 1.3. *The first version of the theorem fits into the approach taken in [LR] and [Sol], while the second fits into the approach taken in [BV20] and [CdSL+19]. Our proof in [BV20] used a conjecture of Bogomolov, Korotiaev and Tschinkel about Jacobians of curves of genus at least two which was proven by Zilber [BKT10, Zil14, Zil17]. In Section 2.2, we extend this conjecture to generalized Jacobians of dimension at least two, and can reverse our argument and use Theorem 3.21 to establish a special case of this extended conjecture.*

Finally, we tackle the general question of recovering the equation of a curve using L -functions of Artin-Schreier extensions.

Theorem 1.4. *For fixed odd prime-power $q = p^r$ and $d \geq 1$, there is an explicit finite set of polynomials $f \in \mathbb{F}_q[x, y]$ such that we can recover the coefficients of any absolutely irreducible $F \in \mathbb{F}_q[x, y]$ of degree d , defining a function field K , from the L -functions of the Artin-Schreier extensions of K given by $z^p - z = f$.*

This is Theorem 4.2. It uses a very large number of L -functions, but can be simplified given additional information about the form of F .

Example 1.5. *The proof of the above theorem shows that we can recover λ in the Legendre family $y^2 = x(x - 1)(x - \lambda)$ over \mathbb{F}_q using the L -functions of the extensions $z^p - z = \alpha x(1 - y^{q-1})$ with α running through a basis of $\mathbb{F}_q/\mathbb{F}_p$. See Example 4.8.*

Acknowledgements. The authors were supported by the Marsden Fund Council administered by the Royal Society of New Zealand. We are grateful for the assistance of Z. Brady for his help with Section 3.4, in particular the proofs of Proposition 3.16 and Lemma 3.24.

2. L-FUNCTIONS AND GENERALIZED JACOBIANS

2.1. Class Field Theory. We describe the well-known connection between the class-field theoretic notions of Hilbert class field and ray class field with the language of generalized Jacobians in the function field setting. Since we wish our extensions to have the same constant field (and have finite degree), we use the version of Hilbert and ray class fields introduced in [Ros87, HK90].

Let K/\mathbb{F}_q be a function field, \mathcal{S}_K be the set of places of K and $S \subset \mathcal{S}_K$ a finite subset. Let I_K denote the ideles of K and $I_{K,S}$ the subgroup of the ideles $(\alpha_v)_{v \in \mathcal{S}_K}$ such that $\alpha_v = 1$ for $v \in S$. We let \mathfrak{m} be a modulus (a formal sum of places of K or, equivalently, an effective divisor) disjoint from S . We allow $\mathfrak{m} = (0)$, the empty divisor. Define $I_{K,S}^{\mathfrak{m}}$ to be the elements of $I_{K,S}$ which are congruent to 1 modulo \mathfrak{m} . The ray class field of K with modulus \mathfrak{m} is defined to be the field corresponding to the subgroup $K^\times I_{K,S}^{\mathfrak{m}}/K^\times$ of I_K/K^\times under the class field theory correspondence. We denote this field by $K_S^{\mathfrak{m}}$.

Lemma 2.1. *The maximal Abelian extension of K in which the places of S split completely and with conductor dividing \mathfrak{m} is $K_S^{\mathfrak{m}}$.*

Proof. This is an extension of [HK90, Theorem (iv)]. Let L be an Abelian extension of K in which the places of S split completely and with conductor dividing \mathfrak{m} . Under the class field theory correspondence, it corresponds to an open subgroup $W \subset I_K$ containing K^\times . For a place $v \in S$, we know that $K_v^\times \subset W$ as v splits completely in L . Since the conductor of L divides \mathfrak{m} , we know that

$$I_{K,S}^{\mathfrak{m}} \subset W.$$

This shows that $K^\times I_{K,S}^{\mathfrak{m}} \subset W$, and hence $L \subset K_S^{\mathfrak{m}}$. □

Now let C be a smooth projective curve over \mathbb{F}_q with function field K . We fix a rational point M of C , and take $S = \{v_M\}$ where v_M is the place associated to M . Note that the splitting condition implies the constant fields of K and $K_S^{\mathfrak{m}}$ are the same.

We consider abelian extension of K (abelian covers of C) such that v_M splits completely (the cover is defined over \mathbb{F}_q and the fiber above M is rational) subject to additional ramification conditions.

Let $J_{\mathfrak{m}}$ denote the generalized Jacobian of C with respect to the modulus \mathfrak{m} [Ser88]. Let $\text{supp}(\mathfrak{m})$ denote the support of \mathfrak{m} , i.e, the set of places of K occurring with nonzero multiplicity in \mathfrak{m} . The Abel-Jacobi map $C \setminus \text{supp}(\mathfrak{m}) \rightarrow J_{\mathfrak{m}}$ associated with a divisor D_1 of degree one is the map $P \mapsto [P - D_1]$. Let Φ denote the Frobenius endomorphism of $J_{\mathfrak{m}}$.

Proposition 2.2. *The ray class field of K with modulus \mathfrak{m} is the function field of the cover C' of C given by the fiber product of the isogeny $\Phi^* - \text{id} : J_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}$ with the Abel-Jacobi map associated to M . This induces an isomorphism $\text{Gal}(K_S^{\mathfrak{m}}/K) \simeq J_{\mathfrak{m}}(\mathbb{F}_q)$ and, viewing $P \in \mathcal{S}_C$ as a divisor of degree $\deg(P)$, the Frobenius Frob_P is identified with $[P - \deg(P)D_1] \in J_{\mathfrak{m}}(\mathbb{F}_q)$.*

Proof. Let L be the function field of C' . Observe that v_M splits completely in L as the fiber of the map $\Phi^* - 1$ over 0 is $J_{\mathfrak{m}}(\mathbb{F}_q)$. We see the cover is Galois, with Abelian Galois group $J_{\mathfrak{m}}(\mathbb{F}_q)$. Furthermore, the conductor of L divides \mathfrak{m} because the cover $C' \rightarrow C \setminus \text{supp}(\mathfrak{m})$ is the pullback of an isogeny $J' \rightarrow J_{\mathfrak{m}}$. Then Lemma 2.1 shows that $L \subset K_S^{\mathfrak{m}}$, so it suffices to show that $J_{\mathfrak{m}}(\mathbb{F}_q) \simeq \text{Gal}(K_S^{\mathfrak{m}}/K)$.

But class field theory in the form of [HK90, Lemma 2 and Theorem] shows that $\text{Gal}(K_S^{\mathfrak{m}}/K)$ is isomorphic to the idele S -ray class group modulo \mathfrak{m} . There is a natural surjection from the

set of divisors on C with support away from \mathfrak{m} to the set of divisors of degree 0 on C whose support is disjoint from \mathfrak{m} given by sending a divisor D to $D - \deg(D)M$. As in [Ser88, V §2], let $C_{\mathfrak{m}}^0$ denote the set of degree zero divisors on C with support disjoint from \mathfrak{m} up to \mathfrak{m} -equivalence; it is a quotient of the group of divisors of degree 0 on C whose support is disjoint from \mathfrak{m} by the divisors of functions on C which are congruent to one modulo \mathfrak{m} . We know that $C_{\mathfrak{m}}^0 = J_{\mathfrak{m}}(\mathbb{F}_q)$, and every equivalence classes of divisors on C with support disjoint from \mathfrak{m} can be represented by a divisor whose support is disjoint from S as well. But the idele S -ray class group modulo \mathfrak{m} is precisely divisors whose support is disjoint from S and \mathfrak{m} modulo the divisors of functions which are congruent to one modulo \mathfrak{m} and are invertible at the points of S . This completes the proof. \square

2.2. L -functions. By a *pointed curve* (C, D_1) , we mean a smooth projective curve C over \mathbb{F}_q together with a choice of degree 1 divisor D_1 . Such a divisor always exists [Sch31]. To connect with class field theory, we assume the existence of a rational point M and take $D_1 = [M]$.

Let χ be a character of $\text{Gal}(K_S^{\mathfrak{m}}/K) \simeq J_{\mathfrak{m}}(\mathbb{F}_q)$ with conductor \mathfrak{m} ; this means \mathfrak{m} is the smallest modulus such that χ factors through $\text{Gal}(K_S^{\mathfrak{m}}/K)$. It is a character of the absolute Galois group of K that is trivial on the absolute Galois group of \mathbb{F}_q .

Definition 2.3. For a place P of K not in $\text{supp}(\mathfrak{m})$, let $\text{Frob}_P \in \text{Gal}(K_S^{\mathfrak{m}}/K)$ denote the Frobenius at P . For any character χ with conductor \mathfrak{m} and $\text{supp}(\mathfrak{m})$ disjoint from S , the L -series (or L -function) for χ is defined as

$$L(T, C, \chi) := \prod_{P \in S_C \setminus \text{supp}(\mathfrak{m})} (1 - \chi(\text{Frob}_P) T^{\deg P})^{-1}.$$

We sometimes use the notation $L(T, D/C, \chi)$ in the case of a Galois cover D/C if we can view χ as a character of $\text{Gal}(D/C)$.

Note that this definition depends on the choice of marked point M as the Abel-Jacobi map determined by M is used to identify the Galois group with $J_{\mathfrak{m}}(\mathbb{F}_q)$. It is a standard calculation that

$$(2.1) \quad \frac{L'(T, C, \chi)}{L(T, C, \chi)} = \sum_{P \in S_C} \frac{(\deg P) \chi(\text{Frob}_P) T^{\deg P - 1}}{(1 - \chi(\text{Frob}_P) T^{\deg P})} = \frac{d}{dT} \left(\sum_{n=1}^{\infty} S_n(\chi) \frac{T^n}{n} \right)$$

where $S_n(\chi) = \sum_{P \in U(\mathbb{F}_{q^n})} \chi(P + \Phi(P) + \dots + \Phi^{n-1}(P))$ and $U = C \setminus \text{supp}(\mathfrak{m})$.

One of the main purposes of this paper is to study the following conjecture:

Conjecture 2.4. Let $(C, [M])$ and $(C', [M'])$ be smooth irreducible projective pointed curves over a finite field \mathbb{F}_q . Let $\mathfrak{m}, \mathfrak{m}'$ be moduli on C, C' with disjoint from M and M' respectively. Suppose the corresponding generalized Jacobians $J_{\mathfrak{m}}, J'_{\mathfrak{m}'}$ have dimension at least two, and that there is a set-theoretic map $\psi : J'_{\mathfrak{m}'}(\overline{\mathbb{F}}_q) \rightarrow J_{\mathfrak{m}}(\overline{\mathbb{F}}_q)$ inducing an isomorphism of groups between $J_{\mathfrak{m}}(\mathbb{F}_{q^n})$ and $J'_{\mathfrak{m}'}(\mathbb{F}_{q^n})$ for every $n \geq 1$. If $L(T, C \otimes \mathbb{F}_{q^n}, \chi) = L(T, C' \otimes \mathbb{F}_{q^n}, \chi \circ \psi|_{J'_{\mathfrak{m}'}(\mathbb{F}_{q^n})})$ for all n and all characters χ of $J_{\mathfrak{m}}(\mathbb{F}_{q^n})$, then C and C' are Frobenius twists of each other and the map ψ arises from a morphism of curves composed with a limit of Frobenius maps which sends M to M' and \mathfrak{m} to \mathfrak{m}' .

Remark 2.5. *More precisely, the last condition means that there exists an integer m , an isomorphism $\alpha : \text{Frob}^m(C) \simeq C'$, and a generalized Frobenius $\beta : \overline{\mathbb{F}}_q \rightarrow \overline{\mathbb{F}}_q$ restricting to Frob^{-m} on \mathbb{F}_q such that $\alpha \circ \beta : C \rightarrow C'$ sends M to M' , \mathfrak{m} to \mathfrak{m}' , and such that $\alpha \circ \beta$ induces ψ on generalized Jacobians.*

Conjecture 2.4 was proved in [BV20] for $\mathfrak{m} = (0)$ as a consequence of a result conjectured by Bogomolov, Korotiaev and Tschinkel [BKT10] and proved by Zilber [Zil14, Zil17]. That result is the $\mathfrak{m} = (0)$ case of the following conjecture.

Conjecture 2.6. *Let $(C, [M])$ and $(C', [M'])$ be smooth, projective, irreducible pointed curves over \mathbb{F}_q and $\mathfrak{m}, \mathfrak{m}'$ moduli on C, C' respectively. Suppose the generalized Jacobians $J_{\mathfrak{m}}$ and $J'_{\mathfrak{m}'}$ have dimension at least two, and let U, U' be the complements of the support of $\mathfrak{m}, \mathfrak{m}'$ in C, C' respectively. If $\psi : J_{\mathfrak{m}}(\overline{\mathbb{F}}_q) \rightarrow J'_{\mathfrak{m}'}(\overline{\mathbb{F}}_q)$ is a group isomorphism such that $\psi(U(\overline{\mathbb{F}}_q)) = U'(\overline{\mathbb{F}}_q)$ (with respect to the Abel-Jacobi embeddings determined by M and M'), then ψ arises from a morphism of curves composed with a limit of Frobenius maps which sends \mathfrak{m} to \mathfrak{m}' .*

More precisely, there exists an integer m , an isomorphism $\alpha : \text{Frob}^m(C) \simeq C'$, and a generalized Frobenius $\beta : \overline{\mathbb{F}}_q \rightarrow \overline{\mathbb{F}}_q$ restricting to Frob^{-m} on \mathbb{F}_q such that $\alpha \circ \beta : C \rightarrow C'$ sends \mathfrak{m} to \mathfrak{m}' and M to M' , and that induces ψ on generalized Jacobians.

The following result relates the two above conjectures.

Theorem 2.7. *Conjecture 2.6 implies Conjecture 2.4. Conversely, assuming Conjecture 2.4, the hypotheses of Conjecture 2.6 and, in addition, that a power of Frobenius commutes with ψ , then the conclusion of Conjecture 2.6 holds.*

Proof. Assume Conjecture 2.4 and, in addition, that the m -th power of Frobenius commutes with ψ . It follows directly that the exponential sums $S_n(\chi)$ for $m|n$ in (2.1) match for each character. Hence (2.1) gives equality of L -functions over extensions of \mathbb{F}_{q^m} and from that we get the morphism.

The proof in the opposite direction is almost verbatim the proof of [BV20, Theorem 2.5] replacing linear equivalence of divisors with the stricter equivalence modulo the fixed modulus. The argument there works without change unless the curves have genus zero. In this latter case, points are linearly equivalent to each other so we need to show that they are not equivalent modulo a fixed modulus under the hypothesis of Conjecture 2.6. Such a modulus has degree at least two.

If two points in \mathbb{P}^1 given by a, b are equivalent modulo \mathfrak{m} and we assume (without loss of generality) that ∞ is in the support of \mathfrak{m} , then we conclude that $(x - a)/(x - b) \equiv 1 \pmod{\mathfrak{m}}$. We distinguish two cases. First assume that there is a point c other than ∞ in the support of \mathfrak{m} . As $(x - a)/(x - b) \equiv 1 \pmod{\mathfrak{m}}$ we see $(c - a)/(c - b) = 1$ and hence $a = b$. If \mathfrak{m} is supported only at infinity, our hypothesis requires $(x - a)/(x - b) \equiv 1 \pmod{2\infty}$. But

$$(x - a)/(x - b) = (1 - a/x)/(1 - b/x) = 1 + (b - a)/x + O(1/x^2)$$

and hence $(x - a)/(x - b) \equiv 1 \pmod{2\infty}$ only if $a = b$. □

Remark 2.8. *In the next section, we will prove a strong form of Conjecture 2.4 when $C = \mathbb{P}^1$ and \mathfrak{m} is a sum of four distinct places of degree one. Under these hypotheses the generalized Jacobians are tori [Ser88, VI §3]. For tori, the \mathbb{F}_q -Frobenius is multiplication by q in the group law so it commutes with ψ automatically. Theorem 2.7 will show that Conjecture 2.6 holds in this case.*

In [BKT10, Theorem 5.11] it was proved that a power of Frobenius commutes with ψ in the case $\mathfrak{m} = (0)$ before conjecture 2.6 was proved for $\mathfrak{m} = (0)$. It would be interesting to see if the argument there can be generalized.

If the generalized Jacobians have dimension one, the condition on the image of the Abel-Jacobi embedding in Conjecture 2.6 is clearly vacuous and the condition on the L -functions in Conjecture 2.4 can also be shown to be vacuous. In the special case that the curves have genus one and both moduli are (0) , [BV20, Remark 2.7] provides examples where the conclusion of both conjectures fail. The other possibility is that the curves have genus zero and the moduli have degree two. In this case, the curves are automatically isomorphic under the conjectures' hypotheses but it is possible to construct group isomorphisms ψ that do not arise from morphisms of curves.

3. THE PROJECTIVE LINE

Let $q = p^r$ be an odd prime power. In this section, we will show how to recover $\mathbb{P}_{\mathbb{F}_q}^1$ with four marked rational points from L -functions of covers unramified away from the marked points.

3.1. Covers of the Projective Line. For $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, consider the modulus

$$\mathfrak{m}(\lambda) = [0] + [1] + [\lambda]$$

on $\mathbb{P}_{\mathbb{F}_q}^1$ and let $U_\lambda := \mathbb{P}_{\mathbb{F}_q}^1 \setminus \{0, 1, \lambda\}$.

Definition 3.1. Let C_λ be the projective curve over \mathbb{F}_q given by the projective equation

$$(3.1) \quad \lambda x^{q-1} - y^{q-1} + (1 - \lambda)z^{q-1} = 0.$$

Let $\pi : C_\lambda \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$ be the map sending $[x, y, z]$ to $[z^{q-1}, z^{q-1} - x^{q-1}]$.

A straightforward calculation checks that C_λ is smooth. Note there is a natural action of μ_{q-1}^3 modulo the diagonal μ_{q-1} , acting by roots of unity on the three coordinates.

Proposition 3.2. The cover $\pi : C_\lambda \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$ is the ray class field cover of $\mathbb{P}_{\mathbb{F}_q}^1$ with respect to $\mathfrak{m}(\lambda)$ in which the infinite place splits completely. In particular,

- (1) π is a degree $(q-1)^2$ branched Galois cover with Galois group μ_{q-1}^2 ;
- (2) there are $q-1$ points of C_λ with ramification index $q-1$ above each point of $\mathfrak{m}(\lambda)$, and the infinite place splits completely;
- (3) over U_λ , π is the pullback of $\Phi^* - 1 : J_{\mathfrak{m}(\lambda)} \rightarrow J_{\mathfrak{m}(\lambda)}$ by the Abel-Jacobi map $U_\lambda \rightarrow J_{\mathfrak{m}(\lambda)}$ which sends t to $[t] - [\infty]$ (as before Φ is the Frobenius map on $J_{\mathfrak{m}}$).

Proof. We know that $J_{\mathfrak{m}(\lambda)}$ is isomorphic to \mathbb{G}_m^3 modulo the diagonal \mathbb{G}_m [Ser88, V §3.13 Prop 7]; hence $J_{\mathfrak{m}(\lambda)} \simeq \mathbb{G}_m^2$ by choosing the first coordinate to be 1. The Abel-Jacobi map sends t to the divisor $[t] - [\infty]$ which is the divisor of the function $f(x) = x - t$. Thus the Abel-Jacobi map is given by sending t to $[(-t, 1 - t, \lambda - t)]$ in $\mathbb{G}_m^3/\mathbb{G}_m$, or equivalently sending t to $(1 - 1/t, 1 - \lambda/t)$ in $J_{\mathfrak{m}(\lambda)} \simeq \mathbb{G}_m^2$. Letting x and y be the coordinates of $J_{\mathfrak{m}(\lambda)}$, as the Frobenius on \mathbb{G}_m is the q th power map pulling back $\Phi^* - 1$ gives the affine curve

$$x^{q-1} = (1 - 1/t), \quad y^{q-1} = (1 - \lambda/t).$$

Eliminating t and writing as a projective equation gives (3.1) and the map π . We directly see the claim about ramification. Note that ∞ splits completely over \mathbb{F}_q as the Abel-Jacobi map sends ∞ to $(1, 1) \in \mathbb{G}_m^2$ and the fiber over $(1, 1)$ is $\mu_{q-1} \times \mu_{q-1}$.

This shows that C_λ is the ray class field cover of $\mathbb{P}_{\mathbb{F}_q}^1$ with respect to $\mathbf{m}(\lambda)$ in which the infinite place splits completely. The Galois group is identified with $J_{\mathbf{m}(\lambda)}(\mathbb{F}_q) \simeq \mu_{q-1}^2$ by having the group act via multiplication by roots of unity on x and y . \square

Corollary 3.3. *The genus of C_λ is $\frac{1}{2}(q-2)(q-3)$.*

Proof. This follows from the Riemann-Hurwitz formula, or the fact that C_λ is a smooth plane curve of degree $q-1$. \square

We now record some additional information about C_λ for use later. Let $G := \mu_{q-1}^2 \simeq J_{\mathbf{m}(\lambda)}(\mathbb{F}_q)$ be the Galois group of π , acting on x and y via roots of unity. Let G_1 (resp. G_λ) be copies of μ_{q-1} embedded into G as the first (resp. second) coordinates, and G_0 be a copy of μ_{q-1} embedded diagonally into G .

Lemma 3.4. *The inertia groups at the $q-1$ points of C_λ over 0 (resp. 1, λ) are G_0 (resp. G_1 , G_λ).*

Proof. Computing using π , we see the points of C_λ over 0 are those with $z = 0$, and hence are fixed by G_0 . The other branch points are similar. \square

Lemma 3.5. *A basis for the space of regular differentials on the projective curve given by an affine equation $ax^{q-1} + by^{q-1} + 1 = 0$ over \mathbb{F}_q is given by $\omega_{i,j} := \frac{x^i y^j}{y^{q-2}} dx$ where $i, j \geq 0$ and $i + j \leq q-4$.*

Proof. This is standard. \square

3.2. L-Functions and the Cartier Operator. Recall that the group $G = \mu_{q-1}^2$ is the Galois group of the cover $\pi : C_\lambda \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$. Given a pair $(b, c) \in \mathbb{Z}/(q-1)$, we define a character $\chi_{b,c} : \mu_{q-1}^2 \rightarrow \mu_{q-1}$ by

$$\chi_{b,c}(\zeta_1, \zeta_2) = \zeta_1^b \zeta_2^c.$$

Any character of G equals $\chi_{b,c}$ for appropriately chosen $(b, c) \in \mathbb{Z}/(q-1)^2$. Let $H_{b,c}$ denote the kernel of $\chi_{b,c}$.

We will use the Cartier operator to obtain information about the L -functions for the cover $\pi : C_\lambda \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$. For our purposes, the Cartier operator may be viewed as a (semi-linear) operator \mathcal{C} on space of regular differentials $H^0(C_\lambda, \Omega_{C_\lambda}^1)$. If $q = p^r$, the r th power of the Cartier operator on C_λ is \mathbb{F}_q -linear and may be computed explicitly using the following result. We define $\alpha_{i,j}$ to be the multinomial coefficient

$$(3.2) \quad \alpha_{m,n} := \binom{q-1}{m, n, q-1-m-n} = \frac{(q-1)!}{m! n! (q-1-m-n)!}.$$

Proposition 3.6. *Let X be the projective curve over \mathbb{F}_q determined by the equation $f(x, y) = ax^{q-1} + by^{q-1} + 1 = 0$ with $ab \neq 0$. Writing $q = p^r$, the r -th power of the Cartier operator acts diagonalizably on $H^0(X, \Omega_X^1)$ with eigenvalues*

$$\alpha_{i+1,j+1} a^{i+1} b^{j+1} \quad \text{for } 0 \leq i, j \text{ with } i + j \leq q-4.$$

The corresponding eigenvectors are $\omega_{i,j} = \frac{x^i y^j}{y^{q-2}} dx$.

Note that the eigenvalues are non-zero if $q = p$ but can be zero when $q \neq p$ as $\alpha_{i+1,j+1}$ may be zero modulo p .

Proof. By [SV87, Theorem 1.1 and proof of Theorem 4.1] the r -th power of the Cartier operator on a regular differential $hf_y^{-1}dx$ (with $h \in \mathbb{F}_q[x, y]$) is given by

$$\mathcal{C}^r(hf_y^{-1}dx) = \left(\left(\frac{\partial}{\partial x} \right)^{(q-1)} \left(\frac{\partial}{\partial y} \right)^{(q-1)} (f^{q-1}h) \right)^{\frac{1}{q}} f_y^{-1}dx$$

where $\left(\frac{\partial}{\partial x} \right)^{(q-1)}$ and $\left(\frac{\partial}{\partial y} \right)^{(q-1)}$ are partial Hasse derivatives. The space of regular differentials of X is $\{hf_y^{-1}dx | h \in \mathbb{F}_q[x, y], \deg h \leq q-4\}$ as in Lemma 3.5.

We will see that the action of \mathcal{C}^r on the basis obtained by taking $h = x^i y^j$ is diagonal. To see this, notice that $\left(\frac{\partial}{\partial y} \right)^{(q-1)}(x^i y^j) = 0$ unless $j \equiv q-1 \pmod{q}$, with a similar statement for the partial Hasse derivative with respect to x . The only term of $f^{q-1}x^i y^j = (ax^{q-1} + by^{q-1} + 1)^{q-1}x^i y^j$ which contributes is the $x^{(i+1)(q-1)}y^{(j+1)(q-1)}$ term of f^{q-1} . Thus we see that

$$\begin{aligned} \mathcal{C}^r(x^i y^j f_y^{-1}dx) &= \left(\left(\frac{\partial}{\partial x} \right)^{(q-1)} \left(\frac{\partial}{\partial y} \right)^{(q-1)} (\alpha_{i+1,j+1} a^{i+1} b^{j+1} x^{(i+1)(q-1)+i} y^{(j+1)(q-1)+j}) \right)^{1/q} f_y^{-1}dx \\ &= \alpha_{i+1,j+1} a^{i+1} b^{j+1} x^i y^j f_y^{-1}dx. \end{aligned} \quad \square$$

The Cartier operator gives significant arithmetic information about smooth projective curves over \mathbb{F}_q , in particular the curve C_λ .

Definition 3.7. The p -rank of C_λ , denoted f_{C_λ} , is the \mathbb{F}_q -dimension of $H^0(C_\lambda, \Omega_{C_\lambda}^1)^{ss}$, the subspace of $H^0(C_\lambda, \Omega_{C_\lambda}^1)$ where \mathcal{C} is invertible.

More generally, for a character $\chi : G \rightarrow \mu_{q-1}$ we define $f_{C_\lambda, \chi} := \dim_{\mathbb{F}_q} H^0(C_\lambda, \Omega_{C_\lambda}^1)^{\chi, ss}$, the dimension of the subspace of regular differentials where \mathcal{C} acts semisimply and $\text{Gal}(C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1) = G$ acts via χ .

We also let $P_\lambda(T, \chi)$ denote the numerator of the Artin L -function $L(T, C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1, \chi)$.

Note that $P_\lambda(T, \chi) = L(T, C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1, \chi)$ unless χ is trivial, in which case $L(T, C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1, 1)$ has a denominator.

Proposition 3.8. Letting $q = p^r$, we have

$$(3.3) \quad P_\lambda(T, \chi) \equiv \det(1 - \mathcal{C}^r T | H^0(C_\lambda, \Omega_{C_\lambda}^1)^\chi) \pmod{p}.$$

In particular, the degree of $P_\lambda(T, \chi)$ is $f_{C_\lambda, \chi}$.

Proof. This is a special case of a result of Rück [Rück86, Theorem 4.1 and Corollary 4.1]. Note that $P_\lambda(T, \chi)$ is a polynomial with coefficients in $\mathbb{Q}(\zeta_{q-1})$; the congruence modulo p is a shorthand for reducing modulo the unique prime above p whose residue field is \mathbb{F}_q . To identify $\mu_{q-1} \subset \mathbb{Q}(\zeta_{q-1})$ with the complex $(q-1)$ -st roots of unity (used to define the L -function) requires an arbitrary choice of an embedding of $\mathbb{Q}(\zeta_{q-1})$ in the complex numbers; we choose one and fix it throughout. \square

Remark 3.9. The result of Rück generalizes a result of Manin [Man61] which relates the numerator of the zeta function with the action of the Cartier operator on the space of regular differentials.

Proposition 3.10. Fix a non-trivial character $\chi_{b,c}$ and let $i := (b - 1 \bmod q - 1)$ and $j := (c - 1 \bmod q - 1)$. If $i + j \leq q - 4$ and $\alpha_{i+1,j+1} \not\equiv 0 \pmod{p}$ then $f_{C,\chi_{b,c}} = 1$ and

$$P_\lambda(T, \chi_{b,c}) \equiv 1 - \alpha_{i+1,j+1} \left(\frac{\lambda}{1-\lambda} \right)^{i+1} \left(\frac{1}{\lambda-1} \right)^{j+1} T \pmod{p}.$$

Otherwise $f_{C,\chi_{b,c}} = 0$ and $P_\lambda(T, \chi_{b,c}) \equiv 1 \pmod{p}$.

Proof. Consider the affine patch of C_λ obtained by taking $z = 1$, given by

$$(3.4) \quad \frac{\lambda}{1-\lambda} x^{q-1} + \frac{1}{\lambda-1} y^{q-1} + 1 = 0.$$

A basis for the regular differentials on C_λ in this coordinate system is given by

$$\omega_{m,n} := \frac{x^m y^n}{y^{q-2}} dx$$

with $m, n \geq 0$ and $m + n \leq q - 4$ by Lemma 3.5. The Galois action of $G = \mu_{q-1}^2$ is acting by roots of unity on x and y , so for $(\zeta_1, \zeta_2) \in \mu_{q-1}^2$ we compute that

$$(\zeta_1, \zeta_2)^* \omega_{m,n} = \frac{(\zeta_1 x)^m (\zeta_2 y)^n}{(\zeta_2 y)^{q-2}} d(\zeta_1 x) = \zeta_1^{m+1} \zeta_2^{n-(q-2)} \omega_{m,n} = \zeta_1^{m+1} \zeta_2^{n+1} \omega_{m,n}.$$

On the other hand, $\chi_{b,c}(\zeta_1, \zeta_2) = \zeta_1^b \zeta_2^c$. Thus $\omega_{m,n}$ lies in $H^0(\Omega_{C_\lambda}^1)^{\chi_{b,c}}$ if and only if $m + 1 \equiv b \pmod{q-1}$ and $n + 1 \equiv c \pmod{q-1}$. Thus we see that $H^0(\Omega_{C_\lambda}^1)^{\chi_{b,c}}$ is one dimensional if and only if $i + j \leq q - 4$. (When this happens, $\omega_{i,j}$ spans the space.)

If $i + j > q - 4$, the dimension of $H^0(\Omega_{C_\lambda}^1)^{\chi_{b,c}}$ is zero and hence $f_{C,\chi_{b,c}} = 0$ and $P_\lambda(t, \chi_{b,c}) = 0$ by Proposition 3.8. If $i + j \leq q - 4$ then Proposition 3.6 shows that

$$\mathcal{C}^r \omega_{i,j} = \alpha_{i+1,j+1} \left(\frac{\lambda}{1-\lambda} \right)^{i+1} \left(\frac{1}{\lambda-1} \right)^{j+1} \omega_{i,j}.$$

By Proposition 3.8, we conclude that

$$P_\lambda(T, \chi_{b,c}) \equiv 1 - \alpha_{i+1,j+1} \left(\frac{\lambda}{1-\lambda} \right)^{i+1} \left(\frac{1}{\lambda-1} \right)^{j+1} T \pmod{p}. \quad \square$$

Corollary 3.11. We have that $P_\lambda(T, \chi_{1,1}) \equiv 1 + 2\lambda(\lambda - 1)^{-2} T \pmod{p}$.

Proof. In this case $i = j = 0$. \square

For λ_1 and $\lambda_2 \in \mathbb{F}_q \setminus \{0, 1\}$ we have identified G as the Galois group of $C_{\lambda_1} \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$ and of $C_{\lambda_2} \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$.

Corollary 3.12. If $L(T, C_{\lambda_1}/\mathbb{P}_{\mathbb{F}_q}^1, \chi_{1,1}) \equiv L(T, C_{\lambda_2}/\mathbb{P}_{\mathbb{F}_q}^1, \chi_{1,1}) \pmod{p}$ then $\lambda_2 = \lambda_1$ or $\lambda_2 = 1/\lambda_1$.

Proof. Let $f(\lambda) = 2\lambda(\lambda - 1)^{-2}$. As $f(\lambda) = f(1/\lambda)$ and $f(\lambda) = c$ has at most two solutions for fixed $c \in \mathbb{F}_q$, this follows from Corollary 3.11. \square

We can remove the ambiguity using a second L -function.

Corollary 3.13. *Suppose $p \geq 5$. If $L(T, C_{\lambda_1}/\mathbb{P}_{\mathbb{F}_q}^1, \chi_{1,1}) \equiv L(T, C_{\lambda_2}/\mathbb{P}_{\mathbb{F}_q}^1, \chi_{1,1}) \pmod{p}$ and $L(T, C_{\lambda_1}/\mathbb{P}_{\mathbb{F}_q}^1, \chi_{1,2}) \equiv L(T, C_{\lambda_2}/\mathbb{P}_{\mathbb{F}_q}^1, \chi_{1,2}) \pmod{p}$, then $\lambda_1 = \lambda_2$.*

Proof. For $b = 1, c = 2$ we have $i = 0$ and $j = 1$, so $i + j = 1 \leq q - 4$ by hypothesis. Using Proposition 3.10 we see that

$$\begin{aligned} P_\lambda(T, \chi_{1,2}) &\equiv 1 - \alpha_{1,2} \left(\frac{\lambda}{1 - \lambda} \right) \left(\frac{1}{\lambda - 1} \right)^2 T \pmod{p} \\ &\equiv 1 - 3\lambda(\lambda - 1)^3 T \pmod{p} \end{aligned}$$

as $i = q - 4$ and $j = 0$ and the exponents only matter modulo $q - 1$. The linear terms of the two pairs of L -functions being congruent modulo p implies that

$$\frac{\lambda_1}{(\lambda_1 - 1)^2} \equiv \frac{\lambda_2}{(\lambda_2 - 1)^2} \pmod{p} \quad \text{and} \quad \frac{\lambda_1}{(\lambda_1 - 1)^3} \equiv \frac{\lambda_2}{(\lambda_2 - 1)^3} \pmod{p}.$$

Hence we conclude that $\lambda_1 = \lambda_2$. □

Remark 3.14. *These corollaries use the non-canonical identification of G with the Galois group of the cover $C_{\lambda_i} \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$ to specify the characters. The identification is natural given the equation (3.1) (and independent of λ), but this is not intrinsic to the curve. To distinguish C_{λ_1} and C_{λ_2} as covers of \mathbb{P}^1 without this non-canonical identification, we must intrinsically identify the character $\chi_{1,1}$. We will address this in the next subsection.*

3.3. Distinguishing Subsets via L -Functions. Let U be an open subset of $\mathbb{P}_{\mathbb{F}_q}^1$ which is the complement of a finite set of \mathbb{F}_q -points P_1, \dots, P_n . If $n \leq 3$, then all such U with n points removed are isomorphic as $\text{PGL}_2(\mathbb{F}_q)$ acts three-transitively on $\mathbb{P}_{\mathbb{F}_q}^1$. If $n = 4$, we wish to determine U up to isomorphism (equivalently, the 4 points up to automorphism of $\mathbb{P}_{\mathbb{F}_q}^1$) using L -functions of characters of covers of U (covers of $\mathbb{P}_{\mathbb{F}_q}^1$ unramified away from P_1, \dots, P_4). We will do so using characters of the ray class field with modulus $[P_2] + \dots + [P_4]$ in which P_1 splits completely. The key technical obstacle is finding a way to specify the character to use.

Proposition 3.15. *Continuing the notation of Section 3.2, if $q \neq 9$ and the character $\chi : \text{Gal}(C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1) = G \rightarrow \mu_{q-1}$ satisfies*

- (1) χ is surjective;
- (2) the genus of $C_\lambda/\ker \chi$ is $(q - 3)/2$;
- (3) the cover $C_\lambda \rightarrow C_\lambda/\ker \chi$ is ramified only at the $q - 1$ points of C_λ lying over 0;
- (4) $f_{C_\lambda, \chi^n} = 1$ if and only if $f_{C_\lambda, \chi_{n,n}} = 1$ for all n such that $0 < 2n < q - 1$;

then χ is $\chi_{1,1}, \chi_{p,p}, \dots$, or $\chi_{p^{r-1}, p^{r-1}}$. If $q = 9$, χ could additionally be $\chi_{1,3}$ or $\chi_{3,1}$.

We can reinterpret (4) using Proposition 3.10. For an integer n , the condition $f_{C_\lambda, \chi_{n,n}} = 1$ is equivalent to the condition $C(n)$ that

$$(3.5) \quad 0 < 2n < q - 1 \quad \text{and} \quad (n \bmod p^i) < p^i/2 \text{ for each } i \in \{1, \dots, r - 1\}.$$

(Note that the first piece of $C(n)$ is almost equivalent to $(n \bmod p^r) < p^r/2$: the only difference is that $n = (p^r - 1)/2$ and $n = 0$ are excluded.) For integers b and c , write $b' = (b \bmod q - 1)$ and $c' = (c \bmod q - 1)$ and let $C(b, c)$ be the condition that

$$(3.6) \quad b' + c' < 2k \quad \text{and} \quad \alpha_{b,c} = \frac{(q - 1)(q - 2) \dots (q - b' - c')}{b'! \cdot c'!} \not\equiv 0 \pmod{p}.$$

Proposition 3.10 shows that $C(nb, nc)$ holds if and only if $f_{C_\lambda, \chi_{b,c}^n} = 1$.

We will prove Proposition 3.15 relying on the following result:

Proposition 3.16. *Let b and c be integers that are relatively prime to $q - 1$ satisfying $0 < b, c < q - 1$. For $0 < n < 2q$, suppose that $C(n)$ holds if and only if $C(nb, nc)$ holds. Then $b = c = p^i$ for some $i \in \{0, 1, \dots, r - 1\}$, or $q = 9$ and $(b, c) = (3, 1)$ or $(1, 3)$.*

We defer the proof of Proposition 3.16 until Section 3.4. The proof is elementary but complicated.

Proof of Proposition 3.15. Suppose χ is a character of G satisfying (1)-(4). As χ is surjective, the degree of the quotient map $C_\lambda \rightarrow C_\lambda / \ker \chi$ is $q - 1$. As this map is Galois, the ramification index of all of the points of C_λ above zero are the same; denote their common value by e . Then the Riemann Hurwitz formula implies that

$$(q - 2)(q - 3) - 2 = (q - 1)(q - 3 - 2) + (q - 1)(e - 1).$$

Thus $e = 2$.

Write $\chi = \chi_{b,c}$ and $H_{b,c} = \ker \chi_{b,c}$. By considering the intersection of the inertia groups given in Lemma 3.4 with $H_{b,c}$, we see that the ramification indices of $C_\lambda \rightarrow C_\lambda / H_{b,c}$ at the points of C_λ above 0 (resp. 1, λ) are $\gcd(b + c, q - 1)$ (resp. $\gcd(b, q - 1)$, $\gcd(c, q - 1)$). Given that $C_\lambda \rightarrow C_\lambda / \ker \chi$ is ramified only at the points over 0 with ramification index 2, we conclude that

$$\gcd(b + c, q - 1) = 2, \quad \gcd(b, q - 1) = 1, \quad \text{and} \quad \gcd(c, q - 1) = 1.$$

Applying Proposition 3.16 and the reformulation of (4) in terms of $C(n)$ and $C(n, n)$, we see that $\chi = \chi_{b,c} = \chi_{1,1}^{p^i}$ for $i \in \{0, 1, \dots, r - 1\}$ unless we are in the exceptional case when $q = 9$. \square

Proposition 3.15 lets us compare L -functions without having to identify the Galois groups.

Theorem 3.17. *Suppose that $q = p^r$ is odd and not equal to 9, and let U and U' be $\mathbb{P}_{\mathbb{F}_q}^1$ with four removed rational points. Fix orderings of the removed points (P_1, \dots, P_4) and (P'_1, \dots, P'_4) . Let C be the ray class field for $\mathbb{P}_{\mathbb{F}_q}^1$ with modulus $\mathfrak{m} = [P_2] + [P_3] + [P_4]$ such that P_1 splits completely. Fix a characters $\chi : \text{Gal}(C/\mathbb{P}_{\mathbb{F}_q}^1) \rightarrow \mu_{q-1}$ such that*

- (1) χ is surjective;
- (2) the genus of the quotient $C/\ker \chi$ is $(q - 3)/2$;
- (3) the cover $C \rightarrow C/\ker \chi$ is ramified only at the $q - 1$ points of C lying over P_2 ;
- (4) $f_{C, \chi^n} = 1$ if and only if $C(n)$ holds for all integers $0 < 2n < q - 1$.

Such a character χ exists, and is “unique up to Frobenius”: the characters $\chi, \chi^p, \dots, \chi^{p^{r-1}}$ are the only characters of $\text{Gal}(C/\mathbb{P}_{\mathbb{F}_q}^1)$ with these properties.

Let C' and χ' be defined analogously for U' . If the derivatives $L'(0, \mathbb{P}_{\mathbb{F}_q}^1, \chi)$ and $L'(0, \mathbb{P}_{\mathbb{F}_q}^1, \chi')$ lie in the same Frobenius orbit of $\mathbb{P}_{\mathbb{F}_q}^1$, in other words there exists an integer $0 \leq i < r$ such that

$$(L'(0, \mathbb{P}_{\mathbb{F}_q}^1, \chi) \pmod{p}) = (L'(0, \mathbb{P}_{\mathbb{F}_q}^1, \chi') \pmod{p})^{p^i},$$

then there is an automorphism α of $\mathbb{P}_{\mathbb{F}_q}^1$ such that $\alpha(U) = U'$, $\alpha(P_1) = P'_1$, and $\alpha(P_2) = P'_2$.

Remark 3.18. *Informally, this says there exists a character $\chi : \text{Gal}(C/\mathbb{P}_{\mathbb{F}_q}^1) \rightarrow \mu_{q-1}$ such that $L(T, C/\mathbb{P}_{\mathbb{F}_q}^1, \chi)$ determines U up to isomorphism. The choice of character is not intrinsic to U as it depends on distinguishing P_1 and P_2 , and is furthermore only unique up to Frobenius. But choosing P_1 and P_2 is sufficient to determine U up to isomorphism as the complement of four points in $\mathbb{P}_{\mathbb{F}_q}^1$ with two of them marked. To remove the restriction on marking two points, one can consider the analogous question after permuting the ordering.*

Proof. Let σ be the fractional linear transformation sending P_1 to ∞ , P_2 to 0, and P_3 to 1. Let $\lambda = \sigma(P_4)$. Then σ induces an isomorphism between C and C_λ as covers of \mathbb{P}^1 as both are ray class fields, and in particular identifies their Galois groups. Proposition 3.15 gives the existence of a character χ with the required properties and shows it is unique up to p th powers as claimed. In particular, there is a $0 \leq j < r$ such that

$$L(T, \mathbb{P}_{\mathbb{F}_q}^1, \chi) = L(T, C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1, \chi_{p^j, p^j}).$$

By Proposition 3.10, we conclude that

$$(L'(0, \mathbb{P}_{\mathbb{F}_q}^1, \chi) \bmod p) = 2 \left(\frac{\lambda}{(\lambda - 1)^2} \right)^{p^j}.$$

We can do the same for U' , obtaining analogous σ' , λ' , and j' .

By hypothesis $(L'(0, \mathbb{P}_{\mathbb{F}_q}^1, \chi) \bmod p) = (L'(0, \mathbb{P}_{\mathbb{F}_q}^1, \chi') \bmod p)^{p^i}$, so there is an integer $0 \leq i' < r$ such that

$$\left(\frac{\lambda}{(\lambda - 1)^2} \right)^{p^{i'}} = \frac{\lambda'}{(\lambda' - 1)^2}.$$

As the function $\lambda \mapsto \lambda(\lambda - 1)^{-2}$ is two-to-one and the p th power map is an automorphism of \mathbb{F}_q , we conclude that $\lambda' = \lambda^{p^{i'}}$ or $1/\lambda' = \lambda^{p^{i'}}$. Thus there is an automorphism β of $\mathbb{P}_{\mathbb{F}_q}^1$ fixing 0 and ∞ and sending $\{1, \lambda\}$ to $\{1, \lambda'\}$; β is either the $p^{i'}$ -th power map or the $p^{i'}$ -th power map composed with the automorphism $x \mapsto x/\lambda$. Then take $\alpha := (\sigma')^{-1} \circ \beta \circ \sigma$. \square

Remark 3.19. *The automorphism $x \mapsto x/\lambda$ sends $\{1, \lambda\}$ to $\{1, 1/\lambda\}$, and corresponds to switching the role of the third and fourth points.*

Remark 3.20. *In the special case that $q = 9$, we can distinguish $U = \mathbb{P}_{\mathbb{F}_q}^1 - \{0, 1, \infty, \lambda\}$ using L -functions as follows. Permuting the four marked points replaces λ by λ , $1/\lambda$, $1 - \lambda$, $1/(1 - \lambda)$, $(\lambda - 1)/\lambda$, and $\lambda/(\lambda - 1)$. Thus there are two choices of U up to isomorphism, which occur when $\lambda = -1$ or when $\lambda \in \mathbb{F}_9 - \mathbb{F}_3$. In light of Proposition 3.10, when $\lambda = -1$ we see that the value $(L'(0, C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1, \chi) \bmod p)$ lies in \mathbb{F}_3 for any character χ . Otherwise there is some character χ for which $(L'(0, C_\lambda/\mathbb{P}_{\mathbb{F}_q}^1, \chi) \bmod p)$ does not lie in \mathbb{F}_3 . Therefore we can distinguish these configurations of points using L -functions.*

We finally prove a strong version of Conjecture 2.4 for the projective line with four marked points. As that conjecture deals with pointed curves, the modulus should be supported on three points.

Theorem 3.21. *Suppose that $q = p^r$ is odd and not equal to 9, and let U (resp. U') be $\mathbb{P}_{\mathbb{F}_q}^1$ with four rational points removed. Fix one of the four points M (resp. M') to define the Abel-Jacobi embedding, and let \mathfrak{m} (resp. \mathfrak{m}') be the sum of the other three. Then let X (resp.*

X') be ray class field of $\mathbb{P}_{\mathbb{F}_q}^1$ in which M (resp. M') splits completely, and let $J_{\mathfrak{m}}$ (resp. $J'_{\mathfrak{m}'}$) be the generalized Jacobian.

Suppose $\psi : J_{\mathfrak{m}}(\mathbb{F}_q) \rightarrow J'_{\mathfrak{m}'}(\mathbb{F}_q)$ is an isomorphism of groups. If

$$L(T, X'/\mathbb{P}^1, \chi') = L(T, X/\mathbb{P}^1, \chi' \circ \psi)$$

for all characters χ' of $J_{\mathfrak{m}'}(\mathbb{F}_q)$, then U and U' are Frobenius twists of each other and the map ψ arises from a morphism of curves which sends M to M' and sends \mathfrak{m} to \mathfrak{m}' .

Proof. Using the $\mathrm{PGL}_2(\mathbb{F}_q)$ -action on $\mathbb{P}_{\mathbb{F}_q}^1$, we may and do assume that $M = M' = \infty$, $\mathfrak{m} = [0] + [1] + [\lambda]$, and $\mathfrak{m}' = [0] + [1] + [\lambda']$ with $\lambda, \lambda' \neq 0, 1$. Note that λ and λ' are not canonical as they depends on the ordering of the removed points. Consider a character χ' of $\mathrm{Gal}(X'/\mathbb{P}^1)$ satisfying conditions (1)-(4) of Theorem 3.17 (with $P_2 = 0$ say) and let $\chi = \chi' \circ \psi$. Let $Y = X/\ker \chi$ and $Y' = X'/\ker \chi'$. We know that $Y' \rightarrow \mathbb{P}^1$ is a cyclic cover of degree $q - 1$ in which ∞ splits and that is ramified only above $0, 1$, and λ' , and that the genus of Y' is $(q - 3)/2$.

Since the zeta functions of Y and Y' are equal by hypothesis, Y also has genus $(q - 3)/2$. We claim that χ also satisfies conditions (1)-(4) Theorem 3.17 (with $P_2 \in \{0, 1, \lambda\}$), which amounts to showing that $Y \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$ is totally ramified at two of $\{0, 1, \lambda\}$ and has ramification index $(q - 1)/2$ at the remaining point. To see this, let the ramification indices at the points of Y above $0, 1$, and λ be $(q - 1)/m_i$ (they divide $(q - 1)$ since the cover is Galois of degree $q - 1$). The Riemann-Hurwitz formula implies that $q - 5 = (q - 1)(-2) + \sum_{i=1}^3 m_i((q - 1)/m_i - 1)$ which simplifies to $\sum m_i = 4$. Thus two are 1 and one is 2. Then the theorem follows from Corollary 3.12 and Proposition 3.15 as in the proof of Theorem 3.17. \square

Remark 3.22. We can also distinguish the projective line with non-rational points removed using L -functions. The simplest approach is to just extend scalars so that all of the points become rational, and use an L -function for a character of the ray class field over \mathbb{F}_{q^n} (with Galois group $\mu_{q^n-1}^2$).

3.4. Proof of Proposition 3.16. We continue to work over a finite field of size $q = p^r$, writing $k := (q - 1)/2$ and assuming $p > 2$. We thank Z. Brady for help with the proofs of Lemma 3.24 and Proposition 3.16; he gave us elegant proofs of version of these results when $r = 1$ (i.e. $q = p$). Our extensions to the case when $r > 1$ have become significantly less elegant, for which we apologize.

We begin with a couple of simple observations about the conditions $C(n)$ and $C(b, c)$ introduced in (3.5) and (3.6).

Lemma 3.23. *We have:*

- (1) condition $C(n)$ holds if and only if $C(k - n)$ holds;
- (2) for $0 < n < q - 1$, the condition $C(n)$ is equivalent to condition $C(n, n)$.

Proof. The first is elementary. For $0 < n < q - 1$, note

$$\alpha_{n,n} = \frac{(q - 1)(q - 2) \dots (q - 2n)}{n! \cdot n!} \equiv \pm \frac{(2n)!}{n! \cdot n!} \pmod{p}.$$

We see $\alpha_{n,n}$ is non-zero modulo p if and only the numerator and denominator have the same p -adic valuation. Since for any positive integer i the number of multiples of p^i less than or equal to $2n$ is at least twice the number of multiples of p^i less than or equal to n , we conclude that $\alpha_{n,n} \not\equiv 0 \pmod{p}$ if and only if the number of multiples of p^i appearing in $(2n)!$ is twice

the number of multiples of p^i appearing in $n!$ for $i = 1, 2, \dots, r-1$. This happens if and only if $(n \bmod p^i) < p^i/2$ for $i = 1, 2, \dots, r-1$. \square

We next need some elementary yet tricky lemmas.

Lemma 3.24. *For any integer b not congruent to $0, 1, p, p^2, \dots, p^{r-1}$ modulo $q-1$, there exists an integer n satisfying $C(n)$ such that $(nb \bmod q-1) \geq (q-1)/2$.*

Proof. Without loss of generality, we may assume that $1 < b < (q-1)/2$ as if $b \geq k = (q-1)/2$ we take $n = 1$. We proceed by induction on r , but treating some special cases by hand. In this proof only, we will use the notation $C_i(n)$ to denote the condition in (3.5) with q replaced by p^i .

For the base case $r = 1$, let $n = \lfloor (k-1)/b \rfloor + 1$, which satisfies $n < (p-1)/2$ as $b > 1$. We directly see that $nb > (k-1) = (q-1)/2 - 1$ and that $nb \leq (k-1) + b < q-1$ as $b < (q-1)/2$.

Next, suppose that $b \not\equiv 0, 1, p, p^2, \dots, p^{r-2} \pmod{p^{r-1}-1}$. By induction, we may suppose that there exists an integer n_0 satisfying $C_{r-1}(n_0)$ such that there are integers a, c for which

$$n_0 b = a(p^{r-1} - 1) + c \quad \text{with} \quad \frac{p^{r-1} - 1}{2} \leq c < p^{r-1} - 1.$$

As $C_{r-1}(n_0)$ holds, we know that $n_0 < (p^{r-1} - 1)/2$ and hence

$$a = \frac{n_0 b - c}{p^{r-1} - 1} < \frac{b - 1}{2}.$$

Then $a(p-1) < b(p-1)/2 - (p-1)/2$ and $(p^r - 1)/2 - (p-1)/2 \leq pc$ and hence

$$(3.7) \quad -b \cdot \frac{p-1}{2} + \frac{p^r - 1}{2} < -(p-1)a + pc.$$

Let ϵ be the smallest positive integer such that

$$\frac{p^r - 1}{2} \leq -(p-1)a + pc + \epsilon b.$$

Then (3.7) shows that $\epsilon \leq (p-1)/2$. Therefore $n := pn_0 + \epsilon$ satisfies $C_r(n)$. We compute

$$bn = (p^r - 1)a - (p-1)a + pc + \epsilon b.$$

By the choice of ϵ and as $b < (p^r - 1)/2$, we conclude that

$$\frac{p^r - 1}{2} \leq -(p-1)a + pc + \epsilon b \leq \frac{p^r - 1}{2} + b < p^r - 1.$$

Thus $(bn \bmod p^r - 1) \geq (p^r - 1)/2$ as desired.

Finally, we directly treat the cases that $b \equiv 0, 1, p, p^2, \dots, p^{r-2} \pmod{p^{r-1}-1}$ where an inductive argument is not possible. We first consider the case when $b = a(p^{r-1} - 1)$ with $a \in \{1, 2, \dots, p\}$. If $a = 1$, take $n = p$. Otherwise take $n = \lfloor (p-1)/(2a) \rfloor + 1$. For both, we see that n satisfies $C_r(n)$ and $(bn \bmod p^r - 1) \geq (p^r - 1)/2$.

In the other cases, write $b = p^i + a(p^{r-1} - 1)$ with $i \in \{0, 1, \dots, r-2\}$ and $0 < a \leq p$.

The case $i = 0$ and $a > 1$: First suppose $b = 1 + a(p^{r-1} - 1)$ with $a > 1$. If $a < p/2$, take $n = p$, and observe that $bn \equiv p + a(1-p) \pmod{p^r - 1}$ so $(bn \bmod p^r - 1) \geq (p^r - 1)/2$.

If $a > p/2$, take $n = 1$ and observe that $b \geq (p^r - 1)/2$. In both cases $C_r(n)$ holds.

The case $a = 1$ and $i > 0$: Now suppose $b = p^i + (p^{r-1} - 1)$ with $i > 0$. Taking $n = cp^{r-i-1} + a$, we compute that

$$bn \equiv 2cp^{r-1} + cp^i - c - cp^{r-i-2}(p-1) \pmod{p^r - 1}.$$

If we choose $c = (p-1)/2$, then we see that

$$2cp^{r-1} + cp^i - c - cp^{r-i-2}(p-1) \leq 2cp^{r-1} + cp^i \leq (p-1)p^{r-1} + \frac{p-1}{2}p^i \leq p^r - 1.$$

We also compute that

$$2cp^{r-1} + cp^i - c - cp^{r-i-2}(p-1) \geq (p-1)p^{r-1} - \frac{p-1}{2} - (p-1)^2p^{r-i-2}/2 \geq (p^r - 1)/2.$$

Thus $(bn \pmod{p^r - 1}) \geq (p^r - 1)/2$ and we directly see that $C_r(n)$ holds.

The case $i > 0$ and $a > 1$: Now suppose $b = p^i + a(p^{r-1} - 1)$ with $a > 1$ and $i > 0$. If $a > p/2$, take $n = 1$. Otherwise, choose $a' = \lceil (p-1)/(2a) \rceil$ and let $n = p^{r-i-1} + a'$. Notice that $C_r(n)$ holds as $a > 1$, and that $(p+1)/2 \leq aa' + 1 \leq p-1$. We compute that

$$bn \equiv p^{r-1} + aa'p^{r-1} + ap^{r-i-2}(1-p) + a'p^i \pmod{p^r - 1}.$$

As $r-i-2 < r-2$ and $i < r-1$, we see that the dominant term in the above expression is $(1+aa')p^{r-1}$. In particular,

$$p^{r-1} + aa'p^{r-1} + ap^{r-i-2}(1-p) + a'p^i \leq (aa' + 1)p^{r-1} + a'p^i < p^r - 1$$

and

$$p^{r-1} + aa'p^{r-1} + ap^{r-i-2}(1-p) + a'p^i \geq (aa' + 1)p^{r-1} - ap^{r-i-2}(1-p) \geq (p^r - 1)/2.$$

Thus $(bn \pmod{p^r - 1}) \geq (p^r - 1)/2$ as desired.

Our argument has covered all of the cases, as we have assumed b is not congruent to $0, 1, p, p^2, \dots, p^{r-1}$ modulo $p^r - 1$. \square

Lemma 3.25. *For odd $q \neq 9$, suppose $b = p^{m_1}$ and $c = p^{m_2}$ with $0 \leq m_1 < m_2 < r$. There exists an integer n for which $C(n)$ does not hold and for which $C(nb, nc)$ holds.*

Proof. Take $n = (p+1)/2$. Notice that $p/2 < n < p$, so $C(n)$ does not hold. On the other hand,

$$\begin{aligned} (nb \pmod{2k}) + (nc \pmod{2k}) &= \frac{p+1}{2}(p^{m_1} + p^{m_2}) \\ &\leq \frac{p+1}{2}(p^{r-1} + p^{r-2}) \\ &\leq p^r \left(\frac{1}{2} + \frac{1}{p} + \frac{1}{2p^2} \right) < q - 1. \end{aligned}$$

The last inequality uses that $p > 3$ or that $p = 3$ and $r > 2$.

Finally we use that $\alpha_{nb, nc} \equiv \pm \frac{((p+1)/2 \cdot p^{m_1} + (p+1)/2 \cdot p^{m_2})!}{((p+1)/2 \cdot p^{m_1})!((p+1)/2 \cdot p^{m_2})!} \pmod{p}$. For $i \leq m_1$, there $(p+1)/2 \cdot p^{m_1-i} + (p+1)/2 \cdot p^{m_2-i}$ multiples of p^i appearing in the factorials comprising the denominator of $\alpha_{nb, nc}$, and a similar number appearing the numerator. For $m_1 < i \leq m_2$ there are $(p+1)/2 \cdot p^{m_2-i}$ multiples of p^i appearing in the denominator and a similar number in the numerator. There are no multiples of p^i appearing when $i > m_2$. Thus the numerator and denominator have the same p -adic valuation, so $\alpha_{nb, nc} \not\equiv 0 \pmod{p}$. \square

We are now ready to prove Proposition 3.16; we again thank Z. Brady for the key idea.

Proof of Proposition 3.16. As b is odd, for any integer n

$$(3.8) \quad A(b, n) := (nb \bmod 2k) + ((k - n)b \bmod 2k) \equiv k \pmod{2k}.$$

In particular, $A(b, n) > 0$.

If $C(n)$ holds, then $C(k - n)$ holds by Lemma 3.23(1). By hypothesis $C(nb, nc)$ and $C((k - n)b, (k - n)c)$ hold as well, so

$$\begin{aligned} 0 < A(b, n) + A(c, n) &= (nb \bmod 2k) + ((k - n)b \bmod 2k) \\ &\quad + (nc \bmod 2k) + ((k - n)c \bmod 2k) < 4k. \end{aligned}$$

As $A(b, n) + A(c, n) \equiv k + k \equiv 0 \pmod{2k}$ and $0 < A(b, n) + A(c, n)$, we conclude that $A(b, n) + A(c, n) = 2k$ if $C(n)$ holds.

We next claim that if $C(n)$ holds then $(nb \bmod 2k) < k$. If $(nb \bmod 2k) > k$, then (3.8) shows that $A(b, n) > 2k$. This is impossible as we know that $A(b, n) + A(c, n) = 2k$ and each term is non-negative. Since b is relatively prime to $2k$ and $n < k$ as $C(n)$ holds, the claim follows.

If b were not a power of p or 1, Lemma 3.24 would give an integer n for which $C(n)$ holds and such that $(nb \bmod 2k) \geq k$, contradicting the claim. Thus $b \in \{1, p, p^2, \dots, p^{r-1}\}$. Likewise, we see that $c \in \{1, p, p^2, \dots, p^{r-1}\}$. Then Lemma 3.25 shows that either $b = c$ or we are in the exceptional case with $q = 9$. This completes the proof. \square

4. GENERAL AFFINE CURVES

Given an equation $F(x, y) = 0$ defining a smooth projective curve C/\mathbb{F}_q , our goal is to recover the coefficients of the equation from an explicit set of L -function for covers of C . We will do so using Artin-Schreier covers. Let K be the function field of C and p the characteristic of K .

4.1. Exponential Sums. We begin by reviewing the connection between L -function for Artin-Schreier extensions and exponential sums; a standard reference is [Bom66, VI].

Artin-Schreier extensions are cyclic degree p extension of K , and are given by the equations $z^p - z = f$ where $f \in K$ is not equal to $w^p - w$ for any $w \in K$. For a fixed f , regular on an open subset U of C , the conductor of E/K is bounded above by $(f)_\infty$, the divisor of poles of f on C .

There is a character $\chi_f : \text{Gal}(E/K) \rightarrow \mathbb{C}^\times$ such that $\chi_f(\text{Frob}_P) = \exp(2\pi i \text{Tr}(f(P))/p)$ for $P \in U$, where Tr is the absolute trace $\text{Tr} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_p$. We assume that E/K is ramified outside U and consider the exponential sums

$$S_m(\chi_f) = S_m(f) := \sum_{P \in U(\mathbb{F}_{q^m})} \exp(2\pi i \text{Tr}(f(P))/p).$$

The values of these sums are determined by $L(T, C, \chi_f)$.

When $p \neq 2$, taking $\varpi = 1 - \exp(2\pi i/p)$ we note that $\mathbb{Z}[\exp(2\pi i/p)]/(\varpi)$ is isomorphic to \mathbb{F}_p and that

$$(4.1) \quad S_m(f) = \sum_{P \in U(\mathbb{F}_{q^m})} (1 - \varpi)^{\text{Tr}(f(P))} \equiv |U(\mathbb{F}_{q^m})| - \left(\sum_{P \in U(\mathbb{F}_{q^m})} \text{Tr}(f(P)) \right) \varpi \pmod{\varpi^2}.$$

If $p = 2$, we instead consider the exponential sums

$$S_m(\chi_{\mathbf{f}}) = \sum_{P \in U(\mathbb{F}_{q^m})} e^{2\pi i T(\mathbf{f}(P))/4}$$

where $\mathbf{f} = (f, 0)$ is a Witt vector of length 2 and $T : W_2(\mathbb{F}_{q^m}) \rightarrow W_2(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$ is the absolute trace (see [VW00]). We can form an L -function as before, which will be a factor of the zeta function of an Artin-Schreier-Witt cover of C . Letting $\varpi = 1 - i$, we get $S_m(\mathbf{f}) \equiv |U(\mathbb{F}_{q^m})| - (\sum_{P \in U(\mathbb{F}_{q^m})} \text{Tr}(f(P)))\varpi \pmod{\varpi^2}$.

Proposition 4.1. *Let $\alpha_1, \dots, \alpha_n$ be a basis for \mathbb{F}_q over \mathbb{F}_p . The L -function $L(T, C, \chi_{\alpha_i f})$ determine the value of*

$$(4.2) \quad T_m(f) := \sum_{P \in U(\mathbb{F}_{q^m})} \text{Tr}_m(f(P)) \in \mathbb{F}_q$$

for each m , where $\text{Tr}_m : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$ is the relative trace.

Proof. We have seen that the knowledge of the L -series $L(T, C, \chi_{\alpha_i f})$ provides us with

$$\sum_{P \in U(\mathbb{F}_{q^m})} \text{Tr}(\alpha_i f(P)) \in \mathbb{F}_p$$

for each m . But these determine $T_m(f)$ as the trace pairing is non-degenerate. \square

4.2. Recovering Affine Equations from Exponential Sums. We now show how to use L -function for appropriate Artin-Schreier covers of a curve to recover the coefficients of a defining equation via considering exponential sums.

Theorem 4.2. *For fixed odd q and $d \geq 1$, there is an explicit finite set of polynomials $f \in \mathbb{F}_q[x, y]$ such that we can recover the coefficients of any absolutely irreducible $F \in \mathbb{F}_q[x, y]$ of degree d from the L -functions of the Artin-Schreier extensions $z^p - z = f$ of the function field K for the curve determined by $F = 0$.*

Remark 4.3. *When q is even we would need the Artin-Schreier-Witt extensions discussed in Section 4.1. Our proof does not apply as written, but we expect it to adapt.*

The proof will use the following lemma about the values of symmetric functions and power sums. For a positive integer n , let e_1, \dots, e_n be the elementary symmetric functions in x_1, \dots, x_n viewed as elements of $\mathbb{Z}[x_1, \dots, x_n]$, and define

$$p_k = \sum_{i=1}^n x_i^k \in \mathbb{Z}[x_1, \dots, x_n].$$

Lemma 4.4. *Fix a field \mathbf{k} of characteristic p . Given $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbf{k}$ and multiplicities n_1, n_2, \dots, n_r with $1 \leq n_i < p$, write $n = \sum_{i=1}^r n_i$. Let β_1, \dots, β_n be these n values, with α_i occurring n_i times. The values of the power sums*

$$p_j(\beta_1, \dots, \beta_n) = \sum_{i=1}^r n_i \alpha_i^j$$

for all j uniquely determine the values of the symmetric functions $e_j(\beta_1, \dots, \beta_n)$ for $1 \leq j \leq n$. If the field \mathbf{k} is a finite field with q elements, it suffices to know the values of the power sums for $j = 1, \dots, q - 1$.

We defer the proof to the next subsection.

Lemma 4.5. *There exists an integer $m > d$ with $p \nmid m$ (depending on q and d only) and an irreducible polynomial $h \in \mathbb{F}_q[x]$ of degree m such that all solutions to $F(x, y) = h(x) = 0$ are defined over \mathbb{F}_{q^m} and that there are $m \deg_y F$ of them. Whether a particular h works can be verified using exponential sums on C .*

Proof. Using Chebotarev, for sufficiently large m there exists an irreducible polynomial $h \in \mathbb{F}_q[x]$ of degree m such that all solutions of $F(x, y) = h(x) = 0$ are defined over \mathbb{F}_{q^m} and there are $m \deg_y F$ of them.

To check this condition for a given irreducible $h \in \mathbb{F}_q[x]$, run through all $s \in \mathbb{F}_q[x]$ with $\deg s < m$ and take $f = (1 - h(x)^{q^m-1})(1 - (y - s(x))^{q^m-1})$. Notice that for $a, b \in \mathbb{F}_{q^m}$ we have $f(a, b) \neq 0$ if and only if $h(a) = 0$ and $b = s(a)$. When $f(a, b)$ is non-zero, it takes on the value 1. If there exists $a \in \mathbb{F}_{q^m}$ such that $h(a) = 0$ and $F(a, s(a)) = 0$, it follows that $F(a^{q^j}, s(a^{q^j})) = 0$ for $j = 1, \dots, m-1$, and hence $F(a, s(a)) = 0$ for all roots a of h in \mathbb{F}_{q^m} . In this case we conclude that $T_m(f) = m^2$ and we have m solutions to $h(x) = F(x, y) = 0$ over \mathbb{F}_{q^m} given by $(a^{q^j}, s(a^{q^j}))$ for $j = 0 \dots m-1$. If not, then $T_m(f) = 0$.

By varying s so that it takes on different values at the roots of h , we can detect whether there are $m \deg_y F$ solutions to $F(x, y) = h(x) = 0$ and that are defined over \mathbb{F}_{q^m} . \square

Lemma 4.6. *Choose h as in Lemma 4.5. For any fixed i, j , there exists $f \in \mathbb{F}_q[x, y]$ such that for $(a, b) \in \mathbb{F}_{q^m}^2$:*

- (1) $z^p - z = f$ is irreducible and the Artin-Schreier extension is ramified over every infinite point of C ;
- (2) if $h(a) \neq 0$ then $f(a, b) = 0$;
- (3) if $h(a) = 0$ then $f(a, b) = a^i b^j$.

The value of $T_m(f)$ can be computed without knowing an explicit choice of f .

Proof. Consider possible f of the form $f = x^i y^j (1 - h^{q^m-1})(1 + (x^{q^m} - x)g)$, for an arbitrary $g \in \mathbb{F}_q[x, y]$. The second and third statements are straightforward to check, and it is clear that the value $f(a, b)$ for $a, b \in \mathbb{F}_{q^m}$ is independent of the choice of g . Thus we must show there is a choice of g such that $z^p - z = f$ is irreducible and the Artin-Schreier extension is ramified over every infinite point of C .

Take a large integer D and consider all functions on K represented by a $g \in \mathbb{F}_q[x, y]$ with $\deg g \leq D$. There are at least $q^{D \cdot d}$ such functions (where $d = \deg F$ as before). For any such g , the resulting f is polynomial of degree at most $D + O(1)$ and is determined, up to a constant, by the polar parts at the places at infinity. If condition (1) is not satisfied, we must have that the polar part at one of the places at infinity is of the exceptional form $w^p - w$ for some Laurent polynomial w at that place. Let v denote the valuation at that place and $m := \min\{v(x), v(y)\}$; note that $0 > m \geq -d/\deg v$. Then $v(f) \geq mD$ and if the polar part of f at v is $w^p - w$ then $v(w) \geq mD/p$ and the coefficients of the powers π^j of a local parameter π at v occurring in the expansion of f for $j < mD/p$ and $p \nmid j$ must vanish. For f to be of this exceptional form at the place v results in at least $D(1 - 1/p)^2$ independent linear conditions on f . As there are at most d such places, we see that there are at most $O(q^{D(1-(1-1/p)^2)})$ polynomials f of degree D for which condition (1) does not hold.

Thus for D sufficiently large (depending just on d and p), we see that at least half of the choices of g must give an f satisfying condition (1). We conclude that the value of $T_m(f)$ for

a choice of f satisfying the first condition is the most common value obtained by computing $T_m(x^i y^j (1 - h^{q^m-1})(1 + (x^{q^m} - x)g))$ for all choices of g with $\deg g \leq D$ and some suitably large D . \square

Proof of Theorem 4.2. By Proposition 4.1, the values of the exponential sums on C are determined by the knowledge of the L -function. Choose m and h as in Lemma 4.5 using our knowledge of the degree of F and of the values of the exponential sums on C . Then choose f as in Lemma 4.6. We compute that

$$T_m(f) = \sum_{\substack{(a,b) \in (\mathbb{F}_{q^m})^2 \\ F(a,b)=0}} \text{Tr}_m(f(a,b)) = \sum_{a:h(a)=0} \sum_{b:F(a,b)=0} \text{Tr}_m(a^i b^j)$$

Since Frobenius cyclically permutes the roots of $h(x)$, we see that

$$T_m(f) = m \sum_{a:h(a)=0} \sum_{b:F(a,b)=0} a^i b^j.$$

As $p \nmid m$, we can use these values with $i = 0, 1, \dots, m-1$ to recover, for each root a of h , the value of $\sum_{b:F(a,b)=0} b^j$ as the Vandermonde matrix is invertible. By Lemma 4.4, these values determine the polynomial $F(a, y) \in \mathbb{F}_q[y]$ for each root a . Viewing $F(x, y)$ as a polynomial in x with coefficients in $\mathbb{F}_q[y]$, the polynomials $F(a, y)$ let us determine $F(x, y) \in \mathbb{F}_q[x, y]$ as $m > d$. This completes the proof. \square

Remark 4.7. *The proof uses a ridiculously large number of L -series of Artin-Schreier covers. It would be nice to have a smaller such set. In specific situations, it is often possible to be more efficient.*

Example 4.8. *Let us use L -function to distinguish members of the Legendre family of elliptic curves $y^2 = x(x-1)(x-\lambda)$. We take $g(x, y) = x(1 - y^{q-1})$. A direct calculation as in the proof shows that*

$$T_1(g) = \sum_{b:b(b-1)(b-\lambda)=0} b = 1 + \lambda.$$

Thus the value of this single exponential sum determines λ .

We now explain how this is an simplification of the proof of Theorem 4.2 for this particular family of curves. First, note that it suffices to recover the coefficient of y in the polynomial $F(x, y) = x^2 - y(y-1)(y-\lambda)$, so we will focus just on recovering the linear term of $F(0, y)$ instead of the whole polynomial. (Note that we swap the usual role of x and y to conform to the notation in our proof.) This polynomial has degree $d = 3$. The assumption in Lemma 4.5 that $m > d$ is irrelevant as we are only interested in the linear term, so let us take $m = 1$. Then $h(x) = x$ satisfies the other conditions of Lemma 4.5 as $0 = x(x-1)(x-\lambda)$ has three solutions over \mathbb{F}_q . Choosing $(i, j) = (0, 1)$, we claim that the $f = y(1 - x^{q-1})$ satisfies the conditions of Lemma 4.6. As f has a pole of order $3q-1$ at infinity, $z^p - z = f$ is irreducible and ramified over the unique point at infinity. If $h(a) = a \neq 0$, then $f(a, b) = b(1 - a^{q-1}) = 0$ and otherwise $f(a, b) = b$ as desired. (Having knowledge of the behavior of x and y at infinity makes finding a suitable f much easier.) This recovers the exponential sum we used above,

$$T_1(f) = \sum_{b:b(b-1)(b-\lambda)=0} b = 1 + \lambda.$$

The proof of Theorem 4.2, which recovers the whole equation, is more complicated as it needs a larger m ; it recovers the coefficient of y in $F(0, y) = -y(y-1)(y-\lambda)$ using Artin-Schreier covers for various (i, j) . In particular, it recovers the coefficient from recovering the sums of powers of the roots 0, 1, and λ . These power sums in turn determine $F(0, y)$.

4.3. Power Sums and Symmetric Functions. It remains to prove Lemma 4.4. Continuing the notation of the lemma, we have the following elementary recurrences:

$$(4.3) \quad ke_k = \sum_{i=1}^k (-1)^{i-1} e_{k-i} p_i \quad \text{when } 1 \leq k \leq n$$

$$(4.4) \quad 0 = \sum_{i=k-n}^k (-1)^{i-1} e_{k-i} p_i \quad \text{when } k > n.$$

These can be deduced cleaning by considering the generating function

$$F(T) = \prod_{i=1}^n (1 - x_i T) = \sum_{i=0}^n (-1)^i e_i T^i.$$

The logarithmic derivative is

$$\frac{F'(T)}{F(T)} = \sum_{i=1}^n \frac{-x_i}{1 - x_i T} = \sum_{j=0}^{\infty} -p_{j+1} T^j.$$

The recurrences follow by cross-multiplying.

For a field K of characteristic zero, $K[p_1, \dots, p_n] = K[e_1, \dots, e_n] = K[x_1, \dots, x_n]^{S_n}$. This is false in positive characteristic (and over \mathbb{Z}).

Example 4.9. Let $p = 2$ and $n = 2$. Then $p_1 = e_1$, and the recurrences tell us that $2e_2 = e_1 p_1 + p_2 = 0$ and that

$$p_3 = e_1 p_2 - e_2 p_1 \quad \text{i.e.} \quad x_1^3 + x_2^3 = (x_1 + x_2)(x_1^2 + x_2^2 - x_1 x_2).$$

Thus we see that

$$e_2 = \frac{p_1 p_2 - p_3}{p_1} \quad \text{i.e.} \quad x_1 x_2 = \frac{(x_1 + x_2)(x_1^2 + x_2^2) - x_1^3 - x_2^3}{x_1 + x_2}.$$

So we can recover the symmetric polynomials as rational functions in p_1, p_2, p_3, \dots (Actually, we just need p_1 and p_3 , as $p_1^2 = p_2$.)

Evaluating at elements of \mathbf{k} , we can recover the values of e_1 and e_2 provided $p_1(x_1, x_2) \neq 0$. This restriction is necessary: consider the family $x_1 = \alpha, x_2 = -\alpha = \alpha$ for $\alpha \in \mathbf{k}$, where we have $p_i(x_1, x_2) = 0$ for all i but $e_2(x_1, x_2) = -\alpha^2$.

Lemma 4.10. For any field \mathbf{k} , the fields $\mathbf{k}(p_1, \dots, p_n, \dots)$ and $\mathbf{k}(e_1, \dots, e_n)$ are equal as subfields of $\mathbf{k}(x_1, \dots, x_n)$.

Proof. As the p_i are symmetric, they may be written as polynomials in terms of the e_i 's. So it suffices to write the e_i as rational functions in terms of the p_i . The key idea is to show that the power series

$$\sum_{j=0}^{\infty} -p_{j+1} T^j$$

is a rational function with coefficients in $k(p_1, p_2, \dots)$. We already know it is a rational function with coefficients in $k(x_1, \dots, x_n)$ from the identity

$$\frac{F'(T)}{F(T)} = \sum_{j=0}^{\infty} -p_{j+1}T^j.$$

As $F(T)$ has no repeated roots, $F(T)$ and $F'(T)$ have no common roots and so if

$$\frac{A(T)}{B(T)} = \frac{F'(T)}{F(T)}$$

with $A(T), B(T) \in k(x_1, \dots, x_n)[T]$ and $A(T)$ of degree at most $n-1$ (in T) and $B(T)$ of degree n (in T), then $A(T) = gF'(T)$ and $B(T) = gF(T)$ for some non-zero $g \in k(x_1, \dots, x_n)$. If we require that the constant term of $B(T)$ is one, then $A(T) = F'(T)$ and $B(T) = F(T)$.

Now write $A(T) = \sum_{i=0}^{n-1} a_i T^i$ and $B(T) = \sum_{i=0}^n b_i T^i$, viewing the a_i and b_i as variables, and consider

$$A(T) = B(T) \cdot \left(\sum_{j=0}^{\infty} -p_{j+1}T^j \right).$$

Equating coefficients of T , we obtain an (infinite) system of linear equation with variables $\{a_i\}$ and $\{b_i\}$ and coefficients in $\mathbf{k}(p_1, p_2, \dots)$. This is solvable over the larger field $\mathbf{k}(x_1, \dots, x_n)$ as we have the identity of rational functions

$$\frac{F'(T)}{F(T)} = - \sum_{j=0}^{\infty} -p_{j+1}T^j.$$

Therefore, the system of linear equations is also solvable over $\mathbf{k}(p_1, p_2, \dots)$.

In particular, there exists $A(T)$ of degree at most $n-1$ and $B(T)$ of degree n in $\mathbf{k}(p_1, p_2, \dots)[T]$ such that

$$\frac{A(T)}{B(T)} = \sum_{j=0}^{\infty} -p_{j+1}T^j.$$

We may certainly scale by an element of $\mathbf{k}(p_1, p_2, \dots)$ so the constant term of $B(T)$ is 1, in which case we must have that $A(T) = F'(T)$ and $B(T) = F(T)$. Therefore the coefficients of $F(T)$, which up to sign are the elementary symmetric functions, lie in $\mathbf{k}(p_1, p_2, \dots)$. This completes the proof. \square

Remark 4.11. It follows from Lemma 4.10 that $\mathbf{k}(p_1, p_2, \dots)$ is generated by finitely many of the p_i 's, although it is not clear which ones do so. As Example 4.9 shows, it is not possible to simply write e_1, \dots, e_n in terms of p_1, \dots, p_n .

We can now prove Lemma 4.4.

Proof of Lemma 4.4. Evaluate F at $x_1 = \beta_1, x_2 = \beta_2, \dots, x_n = \beta_n$, obtaining

$$G(T) := \prod_{i=1}^n (1 - \beta_i T) = \sum_{i=0}^n (-1)^i e_i(\beta_1, \dots, \beta_n) T^i.$$

The logarithmic derivative is

$$\frac{G'(T)}{G(T)} = \sum_{i=1}^r \frac{-n_i \alpha_i}{1 - \alpha_i T} = - \sum_{j=0}^{\infty} p_{j+1}(\beta_1, \dots, \beta_n) T^j.$$

So knowledge of the the power sums determines the rational function $\frac{G'(T)}{G(T)}$. Note that its partial fraction decomposition is unique.

First assume that none of the α_i are zero. The poles of this rational function are the α_i , and the residue at α_i determines n_i modulo p . This is enough to recover the values of the symmetric functions. Otherwise, without loss of generality assume $\alpha_1 = 0$. Then we recover $\alpha_2, \dots, \alpha_r$ and n_2, \dots, n_r , and can find n_1 via $n_1 = n - (n_2 + \dots + n_r)$. \square

Remark 4.12. *Without the restriction that $1 \leq n_i < p$, it is not possible to recover the multiset $\{\beta_1, \dots, \beta_n\}$, as one could add p to one of the n_i and subtract p from another without changing the values of the power sums or the logarithmic derivative of $G(T)$.*

Lemma 4.4 is computationally effective. If all we know is n and the power sums, we can use a continued fraction algorithm on the power series to find the rational function. It is not immediately clear how many power sums are needed in general. If the field \mathbf{k} is the finite field of q elements, then $p_{q-1+i} = p_i$ and thus it's enough to have p_i for $i = 1, \dots, q-1$.

REFERENCES

- [AT09] Emil Artin and John Tate, *Class field theory*, AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original. \uparrow
- [BKT10] Fedor Bogomolov, Mikhail Korotiaev, and Yuri Tschinkel, *A Torelli theorem for curves over finite fields*, Pure Appl. Math. Q. **6** (2010), no. 1, Special Issue: In honor of John Tate., 245–294. \uparrow [2](#), [5](#), [6](#)
- [Bom66] Enrico Bombieri, *On exponential sums in finite fields*, Amer. J. Math. **88** (1966), 71–105. \uparrow [16](#)
- [BV20] Jeremy Booher and José Felipe Voloch, *Recovering algebraic curves from L-functions of Hilbert class fields*, Res. Number Theory **6** (2020), no. 4, 43. \uparrow [1](#), [2](#), [5](#), [6](#)
- [CdSL⁺19] Gunther Cornelissen, Bart de Smit, Xin Li, Matilde Marcolli, and Harry Smit, *Characterization of global fields by Dirichlet L-series*, Res. Number Theory **5** (2019), no. 1, Art. 7, 15. \uparrow [1](#), [2](#)
- [Gaß26] F. Gaßmann, *Bemerkungen zur Vorstehenden Arbeit von Hurwitz: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Math. Z. **25** (1926), no. 1, 661–675, DOI 10.1007/BF01283860. \uparrow [1](#)
- [HK90] Franz Halter-Koch, *A note on ray class fields of global fields*, Nagoya Math. J. **120** (1990), 61–66, DOI 10.1017/S002776300000324X. MR1086569 \uparrow [3](#)
- [LR] W.-C. W. Li and Z. Rudnick, *Pair arithmetical equivalence for quadratic fields*. preprint, arxiv:2007.13147. \uparrow [1](#), [2](#)
- [Man61] Ju. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, Izv. Akad. Nauk SSSR Ser. Mat. **25** (1961), 153–172. \uparrow [9](#)
- [Neu69] Jürgen Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 296–314, DOI 10.1007/BF01425420. \uparrow [1](#)
- [Ros87] Michael Rosen, *The Hilbert class field in function fields*, Exposition. Math. **5** (1987), no. 4, 365–378. MR917350 \uparrow [3](#)
- [Rüc86] H.-G. Rück, *Class groups and L-series of function fields*, J. Number Theory **22** (1986), no. 2, 177–189, DOI 10.1016/0022-314X(86)90068-5. \uparrow [2](#), [8](#)
- [Sch31] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Mathematische Zeitschrift **33** (1931), 1–32. \uparrow [4](#)
- [Ser88] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988. \uparrow [3](#), [4](#), [5](#), [6](#)
- [Sol] P. Solomatin, *On Artin L-functions and Gassmann equivalence for global function fields*. Preprint (2016). <https://arxiv.org/abs/1610.05600>. \uparrow [1](#), [2](#)
- [SV87] Karl-Otto Stöhr and José Felipe Voloch, *A formula for the Cartier operator on plane algebraic curves*, J. Reine Angew. Math. **377** (1987), 49–64. \uparrow [8](#)

- [SV] Andrew V. Sutherland and José Felipe Voloch, *Maps between curves and arithmetic obstructions*. preprint, arxiv:1709.05734, Proceedings of AGCT 16, AMS Contemporary Mathematics, to appear. [↑2](#)
- [Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144, DOI 10.1007/BF01404549. [↑1](#)
- [Uch76] Kôji Uchida, *Isomorphisms of Galois groups*, J. Math. Soc. Japan **28** (1976), no. 4, 617–620, DOI 10.2969/jmsj/02840617. [↑1](#)
- [Uch77] ———, *Isomorphisms of Galois groups of algebraic function fields*, Ann. of Math. (2) **106** (1977), no. 3, 589–598, DOI 10.2307/1971069. [↑1](#)
- [VW00] José Felipe Voloch and Judy L. Walker, *Euclidean weights of codes from elliptic curves over rings*, Trans. Amer. Math. Soc. **352** (2000), no. 11, 5063–5076. [↑17](#)
- [Zil14] Boris Zilber, *A curve and its abstract Jacobian*, Int. Math. Res. Notices **5** (2014), 1425–1439. [↑2](#), [5](#), [23](#)
- [Zil17] ———, *A curve and its abstract Jacobian* (2017). Corrected version of [Zil14], preprint, <http://people.maths.ox.ac.uk/zilber/JacobianCor.pdf>. [↑2](#), [5](#)

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CANTERBURY, PRIVATE BAG 4800, CHRISTCHURCH 8140, NEW ZEALAND

Email address: `jeremy.booyer@canterbury.ac.nz`

URL: <http://www.math.canterbury.ac.nz/~j.booyer>

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CANTERBURY, PRIVATE BAG 4800, CHRISTCHURCH 8140, NEW ZEALAND

Email address: `felipe.voloch@canterbury.ac.nz`

URL: <http://www.math.canterbury.ac.nz/~f.voloch>